

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW HAMPSHIRE**

**UNITED STATES OF AMERICA**

**v.**

**HIEU MINH NGO**

---

)  
)  
)  
)  
)  
)

**1:12-cr-144-PB**

**1:14-cr-081-PB**

**GOVERNMENT’S CONSOLIDATED SENTENCING MEMORANDUM  
AND RESPONSE TO DEFENDANT’S SENTENCING MEMORANDUM  
AND MOTION FOR DEPARTURE/VARIANCE**

**OVERVIEW**

Mr. Ngo has pled guilty to a three-count New Hampshire Superseding Information (1:12-cr-144-PB) charging him with wire fraud, identity fraud and access device fraud, and to a four-count New Jersey Indictment transferred to New Hampshire pursuant to Rule 20 (1:14-cr-81-PB) charging him with hacking into a New Jersey business. The two cases have been consolidated for sentencing.

The facts of this case are not in dispute, although the defendant objects to the loss calculation. The PSI finds a loss to be between \$100,000,000 and \$200,000,000, specifically \$145,901,242, based on 176,000 unauthorized access devices possessed and trafficked by Ngo. In particular, the PSI finds (a) an “intended loss” of \$64,737,742 which is the amount of fraudulent tax refunds sought by criminals who filed tax returns in the names of, and using PII of, innocent victims whose PII was possessed and offered for sale by Ngo, a practice known as stolen identity refund (SIRF) , and (b) what the defendant refers to as “presumed loss” of \$81,163,500 (Id.) which is based upon the number of unauthorized access devices trafficked by Ngo (176,000 minus the 13, 673 which have already been accounted for as being related to the

\$64 million intended loss) multiplied by \$500. Based upon his objections to the Presentence Investigation Report (PSI) and his Sentencing Memo, it appears that the defendant's arguments are as follows: (1) that the sentence range recommended in the PSI, to the extent it is based upon the special rule that provides a minimum loss of \$500 be ascribed to each unauthorized access device, which in this case is slightly more than \$81 million of what he calls "presumed loss," is longer than necessary to achieve the purposes of sentencing and thus violates the "parsimony provision;" (2) that the \$64 million dollars of "intended loss" attributable to 13,673 fraudulent tax filings in the names of victims whose PII the defendant was selling should be eliminated because "there is no evidence that Mr. Ngo intended to cause that amount of pecuniary harm"; and (3) that it is improper to use both "intended loss" and "presumed loss." Although not articulated as such, his memo certainly seems to imply that the sentence range suggested in the PSI substantially overstates the seriousness of the offense. It seems embedded in his argument on "intended loss" at page 11 of his Sentencing Memo.

As addressed below, although the defendant's sentencing arguments are unavailing, it is not the guideline calculation that will ultimately drive the sentence in this case, but rather the sentencing factors set out in 18 U.S.C. § 3553, when considered in light of the extraordinary damage the defendant has caused. Try as we might, unlike with pure economic cyber-crimes such as large scale credit card hacking, in this case, where millions of innocent people's names, addresses, social security numbers, dates of birth, mother's maiden names, bank account numbers, and other PII has been sold into the cyber underworld, from where it can never be retrieved, there is no putting the Genie back in the bottle. Whereas a credit card account can be cancelled and a new card can be issued, it is impossible to reclaim one's stolen PII. In an ironic twist, where the defendant argues that the loss as found in the PSI is too high, in fact, an

argument can be made that is grossly understates the losses he caused, because it focuses only on Ngo's 176,000 stolen "fullz" and ignores the "queries." The vast majority of Ngo's criminal conduct (allowing his 1,300 criminal clients to conduct over 3 million queries of a database containing PII of 200 million U.S. citizens) doesn't figure into the loss calculation, or the sentence range, at all.

Ultimately, whether their "fullz" were sold to Ngo's customers or their PII was queried by Ngo's customers, the millions upon millions of victims in this case, many of whom may not yet know they are victims, could well be subject to years of trying to rehabilitate their credit and reclaim their lives.

## **FACTS**

From 2007 until his arrest in February of 2013, the Defendant Hieu Minh Ngo ("Ngo"), ran a business from his home in Vietnam, through which he sold stolen personally identifiable information ("PII") which can, and in this case did, include individuals' names, dates of birth, addresses, mother's maiden names and social security numbers, and in 176,000 cases, bank account numbers and/or bank routing numbers. He did this, generally, in two ways. First, he ran a web site hosted on a server in the United States through which he allowed his clients, more than 1,300 criminals from around the world, over an 18-month period, to run more than 3 million queries against a U.S. database that contained PII of approximately 200 million U.S. citizens, and then he allowed them to purchase whatever PII they found. Second, in addition to the web site queries, Ngo possessed approximately 176,000 "fullz," which are packets of PII that, in addition to name, date of birth, address, mother's maiden name and social security number, also contain bank account and bank routing information. Ngo trafficked in and sold these "fullz" to his clients upon request. Ngo required all of his clients to maintain a financial

account with Liberty Reserve (LR), an anonymous, virtually untraceable offshore digital currency system. Until taken down by law enforcement, LR was the “bank” of choice for cyber criminals. LR was taken down by law enforcement working out of the Southern District of New York. LR records show that Ngo was paid approximately \$1.75 million for PII by his bad actor clients.

Ngo’s case is important in many respects, but most importantly because it is the first major PII data breach case to be prosecuted. Unlike credit card data breach cases, where the financial losses fall almost exclusively on the banks and/or merchants, a fraudster who is able to obtain PII of innocent, unsuspecting victims is able to engage in many different types of fraud (including bank fraud, credit card fraud and stolen identity refund fraud (SIRF), whereby a fraudulent tax return is filed in an innocent victim’s name claiming a refund that is sent to the fraudster, not the victim), over a lengthy period of time, and their criminal conduct directly impacts individual innocent victims. Unlike when a credit card is compromised, and the bank simply closes the account and issues a new one with the account holder, the account holder victim experiences primarily an inconvenience. By contrast, when a person’s PII is stolen and sold into the underworld of cybercrime, the victim potentially faces years, and in many cases a lifetime, of problems. And the problems can be extremely significant. This is so, because there is nowhere a victim whose PII has been compromised can go to have a new name, address, date of birth, mother’s maiden name or social security number issued. Those pieces of PII are embedded in the average U.S. citizen’s life and for all intents and purposes cannot be changed.

Unlike stolen credit card account information, which becomes valueless as soon as the account is identified as compromised and shut down, a person’s PII is not volatile. A criminal who has a victim’s PII can use it today, or can sit on it and just as effectively use it in a month, or

in a year. Or, worse yet, it can be used for fraud now, and again in a month, and again next year. PII does not expire. The types of fraud perpetrated through the use of stolen PII are limited only by the imagination of the fraudster. Several examples of fraud perpetrated by some of Ngo's clients, who have been convicted in this District and elsewhere, include credit card fraud, bank fraud and SIRF, are discussed below.

#### THE NEW JERSEY CASE

The facts of the New Jersey case are straight forward and are sufficiently set forth in the PSI. Ngo hacked into a business that maintained PII, and he stole PII of more than 5,000 innocent victims so he could sell it to his criminal client base.

#### THE NEW HAMPSHIRE CASE

Having lost his source of PII as a result of the MicroBilt case, Ngo needed another source of stolen PII and ultimately settled on a business in the United States. Although the primary business of that company (business #1) was the aggregation and sale of court records and pleadings from across the country, it had a data sharing agreement with another business in the United States (business #2), a data-aggregation business that collected PII of US citizens for inclusion in its database. This database contained PII of approximately 200,000,000 U.S. citizens. Credit issuing businesses, law enforcement, and private investigators were some of business #1's customers. In essence, the data sharing agreement allowed clients of business #1 to seamlessly access not only the court records of business #1, but the searchable database of business #2, and vice versa.

Ngo misrepresented himself as a private investigator from Singapore to business #1 in order to become a customer of business #1 and thereby, through business #1's data sharing arrangement with business #2, obtain access to run queries of the business #2 database and

obtain PII. Ngo established a website and allowed his 1,300 criminal clients to then access the business #2 database over 3 million times. His customers performed 3 million "queries" of the database, where they would look for and download PII by way of Ngo's contractual relationship with business #1, and the subsequent purchaser of the assets of business #1, another United States company. Ngo was billed 15¢ per query regardless of how much PII his clients downloaded, and Ngo in turn charged his clients per piece of PII they downloaded.

A review of the queries made by Ngo's clients of the business #2 database show that they were looking for PII of individuals from coast to coast and everywhere in between. For example, there were 201,152 queries made of people living in New York, 258,191 queries of people living in Florida, 401,645 queries of people living in California, 46,425 queries of people living in Missouri, and 19,629 queries of people living in New Hampshire.

With no knowledge of the existence of the New Jersey case, the New Hampshire case investigation began in 2011 when US Secret Service Special Agent Matthew O'Neill became aware of a significant multi-national carding website, "findget.me," and its predecessor, "superget.info." A potential purchaser who visited that website was instructed to send an email to a particular email address to obtain a user name and password so the user could open an account. Potential purchasers were required to make payment for purchases through Liberty Reserve. Once logged into Ngo's website, which at that time was named superget.info, a purchaser had the option of buying any number of "fullz" or querying a specific person's name and state of residence to obtain PII of that person, including date of birth, address, social security number and other information. "Fullz" are frequently used by carders to take over the identity of a person in order to engage in various types of fraudulent activities, without the identity theft victim's consent. These can include opening new financial accounts in the victim's name and

making fraudulent purchases on, or transfers of funds from, those accounts; taking out loans in the victim's name; and the filing of fraudulent tax refund requests with the Internal Revenue Service (IRS) on behalf of the victim, a crime known as Stolen Identity Refund Fraud (SIRF). In a SIRF crime, which is a growing problem for the Internal Revenue Service, a fraudster obtains PII of a tax payer and files a fraudulent return in that innocent victim's name seeking a refund. The fraudster then diverts the payment of the refund to himself. Ngo offered several categories of "fullz" for sale, depending on how "fresh" the data was. "Fresher" PII typically cost more than older, less fresh, PII. Although Ngo told his customers he had 500,000 "fullz" after the Secret Service took down the website, a forensic examination disclosed approximately 176,000.

Beginning on November 21, 2011, Agent O'Neill, in an undercover capacity (hereafter UCA), exchanged a series of e-mail messages with Ngo, and he was instructed to open an account at Ngo's web site as well as at Liberty Reserve. The UCA then successfully purchased several hundred "fullz" over the course of several transactions. Although the "fullz" were ordered through the website, typically Ngo sent an email that contained the "fullz" cut and pasted into the text of the e-mail. The "fullz" purchased by the UCA contained several hundred individuals' names, dates of birth, social security numbers, bank routing information, bank account numbers, email account names, and email account passwords. The UCA made it clear during the e-mail exchanges that he was planning to use the "fullz" to try to open credit card accounts in the persons whose names he was buying in the "fullz."

Much of the information contained in Ngo's "fullz," including but not limited to Social Security numbers, constituted Means of Identification as defined at 18 U.S.C. §1028(d)(7).

There is no known legitimate reason to have, or to sell, hundreds of thousands of “fullz.” Each of the “fullz” possessed and sold by Ngo contained information that qualifies as an “access device” and since they were not his, and he did not have legal authority to possess, use or sell them. Accordingly, they were “unauthorized access devices” as those terms are defined in 18 U.S.C. §§ 1029(e).

By way of limited example, Ngo sent three e-mail messages to the UCA containing “fullz” of approximately 245, 50 and 90 individuals. On June 5, 2012, after the UC agent sent an e-mail message to Ngo stating that he wanted to “buy some really fresh fullz for New Hampshire males between 18-40 years. The ones I bought before I couldn’t open credit cards and almost got caught. J how much for 25? How fresh are they?” Ngo sent an e-mail message to the UC agent responding “.5\$ per one info”.

The investigation also uncovered hundreds of other e-mail messages between Ngo and members of his criminal client base that show Ngo negotiating the sale of stolen payment card data and “fullz” to others, containing thousands of “fullz,” including that of many New Hampshire residents. Many examples of Ngo’s sale of stolen credit card data and fullz are set out in the Superseding Information.

## **DEFENDANT’S LOSS CALCULATION ARGUMENTS**

The defendant’s first loss argument is that the Special Rule, found in Application Note 3(F)(i) of USSG Section 2B1.1, should not be used because it would violate the parsimony principle. That Special Rule states:

- (i) Stolen or Counterfeit Credit Cards and Access Devices; Purloined Numbers and Codes.--In a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than \$500 per access device. However, if the unauthorized access device is a means of telecommunications access that identifies a specific telecommunications

instrument or telecommunications account (including an electronic serial number/mobile identification number (ESN/MIN) pair), and that means was only possessed, and not used, during the commission of the offense, loss shall be not less than \$100 per unused means. For purposes of this subdivision, “counterfeit access device” and “unauthorized access device” have the meaning given those terms in Application Note 10(A).

USSG Section 2B1.1(F)(i)(emphasis added).

The Special Rule recognizes that there are cases in which there clearly is harm from the possession, use or trafficking in unauthorized access devices but such harm is not quantifiable. This is either because the harm has not yet occurred, or it has occurred but cannot be ascertained. This happens regularly in the context of cyber-crime where the fraud can be spread around the globe and may never be fully captured for loss determination. The mere fact that the government has not been able to quantify the actual losses should not inure to the defendant’s significant benefit. To do so would be to reward better and more secretive fraud.

In United States v. Alli, 444 F.3d 34 (1st Cir. 2006) the District Court, when confronted with a defendant, a mail carrier who had stolen credit cards with the intent to sell them to a contact in the Netherlands, found the intended loss to be \$88,500, the aggregate credit limit on all of the stolen credit cards. The defendant objected, claiming that, at most, the loss should be capped at \$500 per card, pursuant to the Special Rule in Application Note 3(F). The government agreed with the defendant, wrongly, at sentencing that there was no intended loss. The defendant’s objection was overruled. On appeal the Circuit had to decide “whether a loss that an offender knows will occur, or should reasonably expect to occur, as a direct result of his offense counts as an ‘intended loss’ for purposes of an enhancement under § 2B1.1” *Id.* at 38. Although the Court was not faced with a parsimony principle argument in *Alli*, its holding is instructive. By affirming the District Court, it went well beyond the presumed loss based upon \$500 and found that it was not unreasonable to use the higher credit limit of an unauthorized access device.

In affirming the District Court, the Circuit adopted an objective standard, as opposed to a subjective standard, for determining whether the defendant intended a loss for guideline purposes. That issue will be addressed below as it relates to one of the defendant's other arguments.

Stripped to its core, the defendant's argument really is that when you have large numbers of unauthorized access devices, you necessarily have a loss number that is greater than necessary when considered under the factors in Section 3553(a). That just isn't the case. Each case must be judged on its particular facts. The loss number here, if anything, is too low. As the defendant well knows, the majority of his business, selling access to the database of 200 million U.S. citizens' PII, is not even taken into account in the applicable guideline calculation. Consequently, the Court should overrule his objection.

The second argument advanced is that the intended loss of \$64 million dollars is not proven by the evidence and therefore must be taken out of the calculation. Again he is wrong. The facts as known to the government are as follows. Ngo had 176,000 stolen fullz (packets of PII that contained bank account and bank routing numbers included which made them unauthorized access devices, as defined in 18 U.S.C. § 1029 ), which he in turn sold to his clients. When Ngo's website was taken down there were approximately 176,000 fullz found. Because the government knew many people were using PII from Ngo (fullz and queried PII) to file fraudulent SIF tax returns, the information contained in the fullz was given to the IRS. The IRS then determined that, of the 176,000 fullz of innocent victims Ngo was trafficking in, 13,673 such innocent victims had had SIF returns filed in their names with claimed refunds of slightly more than \$64 million. Because Ngo was trafficking in 176,000 unauthorized access devices, the Probation Department looked to assess loss as to each. With respect to the 13,673 used in

connection with the SIRS returns, the loss was calculated using the fraudulent amount of claimed refunds. Then those 13,763 were subtracted from the total of 176,000 "fullz," and the remaining 162,327 were multiplied by the \$500 Special Rule minimum.

Ngo does not dispute that 13,673 fraudulent returns were filed using PII contained in the fullz he was trafficking in. Rather, he argues that just because he had fullz in the names of the people who had false SIRS returns filed, that doesn't necessarily mean that the false returns were filed by people who bought the fullz from Ngo. In that regard he is technically correct.

Although we cannot prove with certainty that the fullz came from Ngo, we can make a reasonable estimation that Ngo was the source of the 13, 637 fullz. We do know that many people who bought PII from Ngo, including people who have been convicted for using the PII they bought from Ngo, have admitted using it to file SIRS returns. And we are not aware, nor has Ngo offered any information, that any other PII distributor was selling the PII that Ngo had in his cache of fullz.

Without conceding the point, but recognizing that it is a contested issue, and that in the final analysis the guideline calculation, although important, should not be the primary force behind the Court's sentencing decision, if the Court were to decline to use the \$64 million dollar number as it applies to those 13,673 unauthorized access devices, and instead use the Special Rule minimum loss of \$500 for each, the offense level would drop by only 2 levels. As found in the PSI, it is \$145 million, which, because it is between \$100 and \$200 million dollars, results in 26 levels being added. But if the \$500 is applied to all 176,000 fullz, the loss would drop from \$145 million to \$88 million, and the number of levels added for loss would be 24 not 26.

The final argument raised is that somehow the Court should not use a hybrid methodology to determine the loss. That is, the Court should use either the Special Rule as to all,

or should use only identifiable intended loss. Of course, either construction would benefit the defendant, but such is contrary to the plain language of the Rule, which says, in part, “[i]n a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than \$500 per access device.” USSG Section 2B1.1(F)(i)(emphasis added). The government submits that a reasonable interpretation of that Rule calls for exactly what the Probation Department has done. Where there is no identifiable loss use the minimum amount of \$500, but where there is identifiable loss that is greater than \$500, use that as it relates to the specific unauthorized access devices.

#### **DEFENDANT’S DEPARTURE/VARIANCE ARGUMENTS**

In addressing the 3553(a) factors, seeking a below guideline sentence of time served, the defendant suggests that other cases, with distinctly different fact patterns, should weigh too heavily in this Court’s sentencing judgment. At the sentencing hearing the undersigned will, to the extent necessary, point out the differences between Ngo’s case and many of those cited.

Mr. Ngo, unlike many of the “comparable” cases referred to by the defense, has been involved in his life of crime for his entire adult life. And he has never been gainfully employed. His criminal enterprise began at least as early as 2008, and more likely in 2007. Liberty Reserve records reflect that Ngo received funds from his illegal business through two LR accounts. One of them shows that starting on August 7, 2008 Ngo made \$1,750,181.38 through 45,726 separate transactions. In four and one half years his average annual income from his criminal enterprise was \$388,929;  $\$1,750,181.38 / 4.5 \text{ years} = \$388,929$ .

Mr. Ngo was not the inexperienced, impressionable young man his sentencing memo paints him to be. He was the largest seller of stolen PII in the world. SA O’Neill, if he were to

testify, would testify that at the time of Ngo's ongoing business, there was no other source of PII comparable to Ngo. He would add that he still gets emails from former Ngo clients at Ngo's email addresses, asking when he will be back in business and telling him that he was the premier source of PII, anywhere, ever.

### **A Sampling of Ngo's Customers**

To put Ngo's request for a departure or variance in perspective, it is instructive to look at what his clients have done with the PII he sold them, and what sentences they have received, or are likely to receive for their criminal conduct. In follow up investigations, some of Ngo's customers have been charged and convicted for fraud related to the PII they purchased from Ngo, in this District and elsewhere. Although it is a small percentage of Ngo's 1,300 customers, it is a clear and disturbing window into the harm inflicted on innocent victims by Ngo and his clients.

Oluwaseun Adekoya, who was convicted of bank fraud in New Hampshire (1:13-cr-98-JL; 37 months after trial) during a proffer advised that he had a contact at a bank who would give him the names of people who had recently obtained a mortgage. Assuming that people who had just obtained a mortgage had good credit he would then buy the PII of those individuals from Ngo and would then open fraudulent lines of credit in those victims' names at multiple financial institutions. Once the accounts were open he would run the balance up.

Idris Soyemi, who was convicted in this Court (1:13-cr-96-PB; 2 years probation with a 5K1.1 recommendation for testifying at trial) and was part of a fraud group in New York with Mr. Adekoya. He advised that he would obtain stolen cards from a carding forum and then use Ngo's website to obtain PII of the people in whose name the card had been opened and then would get credit reports to determine whether the victim had a high credit score. If so, he would apply for additional credit accounts in that person's name.

Joe Daniels was lured to Boston, arrested and pled guilty (1:13-65-JL; 4 years probation). A review of his email account revealed that he had purchased PII from Ngo. His email account and correspondence with the UCA revealed that he used Ngo's PII to commit traditional forms of identity theft, such as account takeover fraud and establishing new lines of credit as well as creating counterfeit credit cards.

Derric Theoc, who pled guilty in New Hampshire (1:13-cr-64-SM; 27 months) told the UCA that he used the PII he bought from Ngo to commit both tax return fraud and identity fraud. A search warrant of his email account and a review of his Liberty Reserve account confirmed Theoc's statement to the UCA. Based upon an attribution, under the Special Rule, of \$500 loss for each of 625 "fullz" the guideline loss was \$312,500 and the sentencing range was 27 to 33 months. The government recommended the bottom of the range and he was sentenced to 27 months.

Quenten Hall, aka "swipe life," who pled guilty in New Hampshire (1:13-cr-63-PB; 18 months) primarily engaged in traditional forms of identity fraud, but also committed tax return fraud based on a review of his email account. The loss in Hall was calculated to be \$11,000, based upon an attribution of \$500 for each of the 23 "fullz" that he bought from Ngo, and because his conduct involved trafficking in unauthorized access devices a 2-level enhancement was recommended. Quenten Hall, who purchased 23 "fullz" was sentenced by this Court to serve 18 months in prison.

Lance Ealy, who was referred to the Secret Service in Ohio for prosecution, engaged in fraudulent tax filings as well as aggravated identity theft and credit card fraud. He was convicted after a trial at which Ngo testified for the government. Ealy has not been sentenced, but the AUSA handling the case has advised that his total offense level is 31 and that with a Criminal

History Category of III his advisory guideline range is 135-168 prior to a mandatory consecutive 24 month sentence. The SIRC returns he filed were done in the names of people whose PII he had purchased from Ngo.

Additionally, three individuals from Texas have been indicted in this District for allegedly filing fraudulent tax returns in victims' names whose PII they purchased from Ngo. They are pending trial currently.

Although this is a relatively small sample size, this group of Ngo's confederates allow one to see the actual harm that is done with the PII sold by Ngo. These cases, and the sentences meted out, also show the unfairness and inequitable nature of Ngo's suggestion that he be sentenced to time served. He was the king pin of the operation. He sold the criminal tradecraft, on a piecemeal basis, to his minions, who then used that PII to commit further crime. His buyers, who possessed only a tiny fraction of the quantity of PII that Ngo trafficked, received sentences in the range of that which asks this Court to give him.

## **CONCLUSION**

### **15 Years is an Appropriate Sentence**

The 15-year sentence being recommended by the government is appropriate based on the guideline calculation, as well as on the factors set out in 3553(a). It is also in line with other sentences handed down recently in other, somewhat similar hacking/carding prosecutions, particularly in light of the fact that as serious as credit card hacking is, the real world impact it has on real people is relatively minor as compared to what Ngo has done. In 2013, in the Western District of Washington, David Schrooten, 22, was sentenced to 12 years for a carding scheme involving only 100,000 compromised cards and only two hacked businesses. In that case, his co-conspirator, Christopher Schroebel, 21, who had been the hacker, was sentenced to 7

years. In the District of New Hampshire, Adrien Oprea, who ran a hacking scheme that stole credit card data from restaurant point of sale terminals was sentenced to 15 years.. In 2012, in the Eastern District of New York, Aleksandr Suvorova was sentenced to 7 years for hacking into 11 restaurants and selling 160,000 stolen cards to an undercover agent. In November 2011, also in the Eastern District of new York, Lin Mun Poo was sentenced to 10 years for a hacking and carding scheme involving 120,000 stolen credit cards. In 2012, in the Eastern District of Virginia, Peter Borgia, 22, was sentenced to four years for a carding scheme involving only 21,000 stolen cards and \$3 million in losses. In February of 2010 Max Ray Vision, aka Max Butler was sentenced to 13 years in prison after stealing 1.8 million credit card numbers. Alberto Gonzalez, who was the ring leader of the TJX retail hack was sentenced to 20 years after he and his accomplices stole more than 90 million credit card accounts. Finally, in Nevada in May of 2014, David Ray Camez was sentenced to 20 years in prison for his role in a multi-national ring involved in buying and selling personal information and stolen credit cards.

A 15-year sentence in this case would also be in line with other sentences meted out in other cases related to this case. As is reflected above, people to whom relatively small amounts of PII was sold by Ngo have been, and will be, sentenced to significant prison terms.

### **Just punishment, respect for law, deterrence, and public protection**

A sentence of 180-months would serve both specific and general deterrence goals. Ngo's crime was not a one-time, impulsive crime; rather, he engaged in a prolonged and methodical multi-year crime spree. So a significant prison sentence is needed to deter Ngo and to send a message to other hackers.

The need for deterrence is especially acute with computer hackers and other cyber-criminals.

As Judge Gertner stated in United States v. Watt:

[C]ybercrimes by their very nature allow offenders to commit the offenses without leaving their homes and with a veil of anonymity. This lack of contact with the victims of their crimes and insulation from law enforcement may cause them to be under-deterred. Only successful prosecution and significant punishment will supply prospective cyber-criminals with the information needed to create real deterrence.

707 F.Supp.2d 149, 156-57 (D.Mass. 2010).

Donald Feith  
Acting United States Attorney

June 12, 2015

By: /s/ Arnold H. Huftalen  
Arnold H. Huftalen  
Assistant U.S. Attorney  
Bar Association # 1215  
53 Pleasant St., 4th Floor  
Concord, NH 03301  
arnold.huftalen@usdoj.gov  
(603) 225-1552

Certificate of Service

I certify that a copy of this Memorandum has been served upon the defendant, through counsel, via ECF Filing Notice today, June 12, 2015.

By: /s/ Arnold H. Huftalen  
Arnold H. Huftalen  
Assistant U.S. Attorney